VZCZCXRO4730
RR RUEHFL RUEHKW RUEHLA RUEHNP RUEHROV RUEHSR
DE RUEHMO #3590 3471055
ZNY CCCCC ZZH
R 121055Z DEC 08
FM AMEMBASSY MOSCOW
TO RUEHC/SECSTATE WASHDC 1105
INFO RUCNCIS/CIS COLLECTIVE
RUEHZL/EUROPEAN POLITICAL COLLECTIVE
RUEKJCS/JOINT STAFF WASHDC
RUEKJCS/SECDEF WASHDC
RHEHNSC/NSC WASHDC
RUEAIIA/CIA WASHDC

C O N F I D E N T I A L MOSCOW 003590

SIPDIS

E.O. 12958: DECL: 12/11/2018
TAGS: PREL EINT TINT MOPS PINR RS
SUBJECT: RUSSIA DENIES CYBER-ATTACKS

Classified By: Acting DCM Alice G. Wells for reasons 1.4 (b) and (d).

¶1. (C) Summary: The Russian MFA issued a strong denunciation on December 4 of press reports accusing Russia of attacks on the DoD's classified computer network and of denial of service attacks on Georgia and Estonia. The GoR has not yet responded to December 10 press accusations and statements by Secretary Chertoff. Despite official Russian denials, the Russian press has openly discussed Russian-originated cyber-attacks on Georgia during the August conflict, though reportedly as a response to Georgian-originated attacks: while one ruling party Duma member described a private initiative to target Estonia. Despite the MFA's statement which called cooperation in combating cyber-assaults a promising area for bilateral U.S.-Russia relations, we note that Russia has failed to agree to participate in joint training or conferences on the issue. End summary.

¶2. (SBU) On December 4, Russia issued a strong denunciation of press reports that tied it to attacks on the Pentagon's classified computer network. "In conditions of global computerization and the growing common threat of the use of information technologies for unfriendly purposes, such informational leaks are not only groundless, but also irresponsible," said a statement posted on the MFA website. The ministry also refuted linkage of Russia to "denial of service" attacks on Estonia and Georgia. The MFA statement instead pointed to the U.S. for failing to support a Russian draft text on the subject at the 63rd UNGA, saying "characteristically, the U.S. alone voted against this resolution." However, it also called for greater U.S.-Russia bilateral cooperation -- the "assurance of international information security could be a promising direction for our partner dialogue with the United States as well."

¶3. (SBU) The GOR has yet to respond to a new accusation reported in Fox News and public comments by Homeland Security Secretary Chertoff December 10. Fox News accused a Russian front company, "run by several former Russian KGB or Federal Security Service (FSB) spies," of mounting recent attacks on the DoD's classified network, reporting that the company inserted a "worm" into a U.S. forces Afghanistan system by means of an external hardware device (e.g., a flash drive). Chertoff was reported to have said that "there was a preceding effort in denial of service...by let us say sympathizers to the Russian side of the dispute." Chertoff also reportedly called for a doctrine to determine when a cyber-attack constituted an act of war.

¶4. (SBU) Despite the public denials, the Russian media has openly discussed the coordinated attacks from Russia on Georgian websites during the August conflict. In an October 29 article carried on the Novyy Region wire service, the author accused Georgia of bringing down South Ossetian websites and attempting to take out Russian news media sites.

In response, he noted that "retaliatory steps were not long in coming," and credited Russian hackers for bringing down the websites of President Saakashvili, the Georgian parliament, the government, and the Foreign Ministry in denial of service attacks. "President Saakashvili's website came under (denial of service) attacks from 500 IP addresses simultaneously" the article stated.

¶5. (C) One prominent ruling party Duma member, Sergey Markov, assured to us there were Russian cyber-attacks, but they were not officially sanctioned. Markov claimed in a December 11 meeting that his own assistant, working with hackers in Transnistria, orchestrated the cyber-attack on Estonia. He said the assistant had taken the steps on his own, without prior consultation with Markov, because he was so reviled by the wartime statue issue in Estonia.

¶6. (C) Comment: Despite the MFA's calls for closer, cooperative efforts in cyber-security, the GOR declined LEGATT's invitation to attend a large January 2009 cyber-security conference in New York or to attend other training opportunities. There presently is no meaningful cooperation with the GOR on this issue at Post, although there is extensive cooperation with the FSB and Ministry of Internal Affairs on cyber-crime cases. While cyber-security could develop into an excellent path for bilateral cooperation, close coordination may also provide Russian special services an opportunity to assess U.S. technical limitations and investigative techniques.
RUBIN